RANDOM-NUMBER GENERATING CIRCUIT, NONCONTACT IC CARD AND READER/WRITER HAVING SAME RANDOM-NUMBER GENERATING CIRCUIT INSIDE, AND METHOD FOR TESTING DEVICE HAVING SAME RANDOM-NUMBER GENERATING CIRCUIT INSIDE

Publication number: JP2000222176

Publication date: 2000-08-11

Inventor: FUJIOKA SOZO

Applicant: MITSUBISHI ELECTRIC CORP; MITSUBISHI DENKI SYS LSI DES

Classification:

- international: ***G06K19/10; G06F1/02; G06F7/58; G06K17/00; G09C1/00;*** **G06K19/10; G06F1/02; G06F7/58; G06K17/00; G09C1/00;** (IPC1-7): G06F7/58; G06K17/00; G06K19/10; G09C1/00

- European: G06F7/58P1

Application number: JP19990026369 19990203

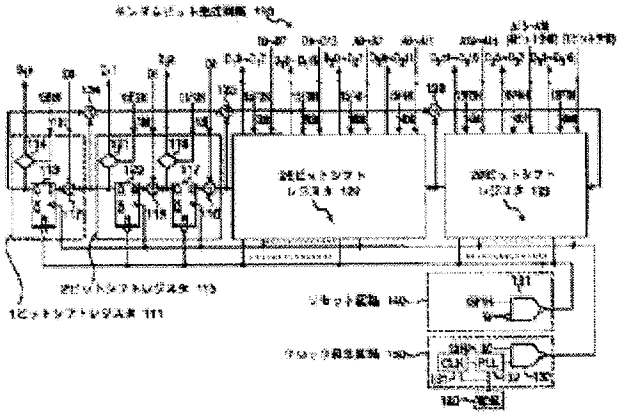
Priority number(s): JP19990026369 19990203

Also published as:

US 6480869 (B1)

Abstract of **JP2000222176**

PROBLEM TO BE SOLVED: To generate random number data which are irregular and hardly predicted and to generate the random number data fast with simple constitution by generating the random number data by making use of bit data sent through an external signal line. SOLUTION: A random-bit generating circuit 110 adds bit data which changes with time according to process contents to be executed by a CPU to respective bit data stored in a 1-bit shift register 111, a 2-bit shift register 115, a 25-bit shift register 122, and a 20-bit shift register 123 constituting what is called a 48-bit M-series random number generating circuit. Namely, the respective bit data A0 to A19 of a 20-bit address signal sent through a system bus, the respective bit data D0 to D15 of a 16-bit data signal, and the respective bit data of 12 bits in total composed of other signals are added respectively. The 3 bytes obtained by the addition, i.e., data D10 to D115, D20 to D215, and D30 to D316 of 48 bits in total are outputted as random number data.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－222176
（P2000－222176A）
(43)公開日　平成12年８月11日(2000.8.11)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　7/58		Ｃ０６Ｆ　7/58	Ａ	５Ｂ０３５
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｔ	５Ｂ０５８
19/10		Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６５０	Ｃ０６Ｋ　19/00	Ｒ	９Ａ００１

審査請求　未請求　請求項の数７　ＯＬ　（全 13 頁）

(21)出願番号　特願平11－26369

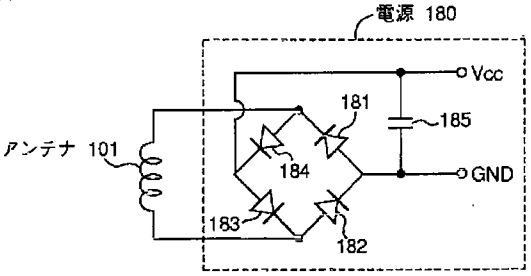
(22)出願日　平成11年２月３日(1999.2.3)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(71)出願人　391024515
三菱電機システムエル・エス・アイ・デザイン株式会社
兵庫県伊丹市中央３丁目１番17号
(72)発明者　藤岡　宗三
兵庫県伊丹市中央３丁目１番17号　三菱電機システムエル・エス・アイ・デザイン株式会社内
(74)代理人　100062144
弁理士　青山　葆　（外２名）

最終頁に続く

(54)【発明の名称】　乱数生成回路、当該乱数生成回路を内蔵する非接触ＩＣカード及びリーダ／ライタ、並びに、当該乱数生成回路を内蔵する装置のテスト方法

(57)【要約】
【課題】　簡単な構成で、かつ、高速に精度の高い乱数を発生する乱数生成回路を提供する。
【解決手段】　本発明の乱数生成回路は、カスケード接続された１以上のビットのクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の少なくとも１組のシフトレジスタの出力の合計を求め、求めた合計のデータを所定のシフトレジスタの入力端子に入力する加算回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とで構成される乱数生成回路であって、上記複数のシフトレジスタの内の１以上のシフトレジスタは、格納しているビットデータの内の１以上のビットデータに外部信号線に流れるビットデータを加算する加算手段と、上記加算手段による加算後に、格納しているビットデータの内の１以上の所定のビットデータを乱数データとして出力する出力手段とを備えることを特徴とする。



【特許請求の範囲】

【請求項１】　カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の２以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、

上記複数のシフトレジスタの内の１以上のシフトレジスタは、外部信号入力端子と、格納しているビットデータの内の１以上のビットデータに上記外部信号入力端子を介して入力されるビットデータを加算する加算回路とを備え、加算回路による加算後のビットデータを乱数データとして出力することを特徴とする乱数生成回路。

【請求項２】　カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の２以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、

上記クロック発生回路は、所定の周波数のクロック信号を生成するＣＬＫ回路と、上記ＣＬＫ回路により生成されたクロック信号を基準周波数信号として受け取るＰＬＬ回路とで構成され、上記ＰＬＬ回路の出力を上記各シフトレジスタに出力することを特徴とする乱数生成回路。

【請求項３】　請求項１又は請求項２に記載の乱数生成回路において、

上記シフトレジスタを構成するクロック同期型のフリップフロップは、電源投入時に出力するデータを”Ｈ”とする第１構成要素と、第１構成要素と同一のドライブ能力を有し、電源投入時に出力するデータを”Ｌ”とする第２構成要素とを備え、上記第１及び第２構成要素の出力端子には、それぞれ同一の容量の配線及びトランジスタが接続されていることを特徴とする乱数生成回路。

【請求項４】　請求項１乃至請求項３の何れかに記載の乱数生成回路において、

更に、リセット要求信号の入力に応じて各シフトレジスタにリセット信号を出力するリセット回路を備え、

上記クロック発生回路は、クロック停止信号の入力に応じてクロック信号の各シフトレジスタへの出力を停止し、クロック動作信号の入力に応じてクロック信号を各シフトレジスタへ出力する論理回路を備えることを特徴とする乱数生成回路。

【請求項５】　請求項１乃至請求項４の何れかに記載の乱数生成回路を内蔵する非接触ＩＣカードであって、当該非接触ＩＣカード用リーダ／ライタとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする非接触ＩＣカード。

【請求項６】　請求項１乃至請求項４の何れかに記載の乱数生成回路を内蔵する非接触ＩＣカード用リーダ／ライタであって、対応する非接触ＩＣカードとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする非接触ＩＣカード用リーダ／ライタ。

【請求項７】　請求項４に記載の乱数生成回路を内蔵し、当該内蔵する乱数生成回路から出力される乱数データを用いて所定の処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されている装置のテスト方法であって、クロック発生回路から所定の周波数のクロック信号が出力されている状態において、クロック発生回路の論理回路にクロック停止信号を出力し、リセット回路にリセット要求信号を出力した後に、クロック発生回路の論理回路にクロック動作信号を出力すると同時に上記装置のテスト処理を実行し、上記テスト処理の完了と同時にクロック発生回路の論理回路にクロック停止信号を出力し、出力手段より出力される乱数データの値を読み取り、読み取った乱数データと基準データとの比較により、システムの異常検出を行うことを特徴とする装置のテスト方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、乱数生成回路、特に、非接触ＩＣカード及び当該非接触ＩＣカードのリーダ／ライタに用いる乱数生成回路に関する。

【０００２】

【従来の技術】近年、インテリジェント機能や書き換え可能なメモリ機能を備える薄型の非接触ＩＣカードが数多く提供されている。非接触ＩＣカードは、リーダ／ライタに接続させることなくデータのやり取りができることを特徴とする。非接触ＩＣカードは、例えば、プリペイドカード、ドアの鍵、電車やバスなどの定期券、スキーのリフト券等に用いられる。

【０００３】非接触ＩＣカードに書き込まれているデータの不正流出や改竄を防止するため、上記非接触ＩＣカードと当該カードのリーダ／ライタは、データのやり取りを行う前に、互いを認証する処理を実行する。リーダ／ライタは、自己の発信するポーリング信号に対して所定のレスポンス信号を返信してきた非接触ＩＣカードとの間で相互認証処理を実行する。相互認証処理の方法としては、暗号化鍵を用いる方法が知られている。

【０００４】以下、非接触ＩＣカードとリーダ／ライタ

との間で行う暗号を用いた相互認証処理について簡単に説明する。まず、リーダ／ライタは、非接触ＩＣカードに対して内部で生成した乱数ａを送信する。非接触ＩＣカードは、受信した乱数ａを自己の暗号化鍵を用いて乱数Ａに変換し、乱数Ａをリーダ／ライタに返送する。リーダ／ライタでは、特定の非接触ＩＣカードとの間で用いる共通の暗号化鍵を用いて上記生成した乱数ａを処理して乱数Ａ'を求め、求めた乱数Ａ'と上記非接触ＩＣカードから返送されてきた乱数Ａとを比較する。リーダ／ライタは、乱数Ａと乱数Ａ'が一致する場合に当該非接触ＩＣカードを正規のものであると認証する。

【０００５】次に、非接触ＩＣカードはリーダ／ライタに対して内部で生成した乱数ｂを送信する。この場合、リーダ／ライタは、受信した乱数ｂを自己の暗号化鍵を用いて乱数Ｂに変換し、乱数Ｂを非接触ＩＣカードに返送する。非接触ＩＣカードは、特定のリーダ／ライタとの間で用いる共通の暗号化鍵を用いて上記生成した乱数ｂを処理して乱数Ｂ'を求め、求めた乱数Ｂ'と上記リーダ／ライタから返送されてきた乱数Ｂとを比較する。非接触ＩＣカードは、乱数Ｂと乱数Ｂ'が一致する場合に当該リーダ／ライタを正規のものであると認証する。

【０００６】非接触ＩＣカード及びリーダ／ライタ内には上記相互認証処理で用いる乱数を生成する乱数生成回路が内蔵されている。図１０は、従来より用いられている乱数生成回路５００の回路図である。乱数生成回路５００は、いわゆる４８ビットＭ系列乱数生成回路と呼ばれる回路であり、カスケード（多段直列）接続された１ビットシフトレジスタ５０１、２ビットシフトレジスタ５０４、２５ビットシフトレジスタ５０５及び２０ビットシフトレジスタ５０６、並びに、各ビットシフトレジスタの出力の合計を初段の２０ビットシフトレジスタ５０６の入力端子に入力する加算回路を構成する加算器５０７、５０８及び５０９で構成される。

【０００７】１ビットシフトレジスタ５０１は、ＣＬＫ回路５１０より出力されるクロック信号ＣＬＫに同期して動作するフリップフロップ５０２及びトランスファーゲート５０３により構成される。図示しないＣＰＵによりアドレス０２Ｅ２Ｈが選択されアドレス信号線が”Ｌ”から”Ｈ”に切り換わった時にフリップフロップ５０２の出力を乱数データ$D_1 0$として出力する。

【０００８】２ビットシフトレジスタ５０４，２５ビットシフトレジスタ５０５及び２０ビットシフトレジスタ５０６の回路は、各々シフトするビット数だけ上記１ビットシフトレジスタ５０１と同じ回路を直列に接続したものである。２ビットシフトレジスタ５０４は、アドレス１５Ｆ２Ｈが選択された時に乱数データ$D_1 1$、$D_1 2$を出力する。２５ビットシフトレジスタ５０５は、アドレス１５Ｆ２Ｈ、１５Ｆ３Ｈ、１５Ｆ４Ｈ及び１５Ｆ５Ｈが選択された時に乱数データ$D_1 3$～$D_1 7$、$D_1 8$～$D_1 15$、$D_2 0$～$D_2 7$及び$D_2 8$～$D_2 11$を出力する。２０ビットシフトレジスタ５０６は、アドレス１５Ｆ５Ｈ、１５Ｆ６Ｈ及び１５Ｆ７Ｈが選択された時に乱数データ$D_2 12$～$D_2 15$、$D_3 0$～$D_3 7$、$D_3 8$～$D_3 15$を出力する。

【０００９】

【発明が解決しようとする課題】上記構成の乱数生成回路５００の生成する乱数は、一定の周期で繰り返す所定の生成パターンを有する。このため、リーダ／ライタと非接触ＩＣカードとの間でやり取りされる通信データが盗聴され、乱数の生成パターンが特定される場合がある。このように乱数の生成パターンが特定されると、暗号化鍵や暗号化処理の内容が解らずとも、乱数ａと乱数Ａを対応づけたテーブルを用いることで非接触ＩＣカードを偽造することができる。同様に、乱数ｂと乱数Ｂを対応づけたテーブルを用いることでリーダ／ライタの偽造を行うことができる。

【００１０】上記通信データの盗聴による非接触ＩＣカードやリーダ／ライタの偽造を有効に防止するには、通信データを盗聴しても生成パターンを解読できない程の高度な乱数生成回路が要求される。しかし、乱数生成回路を複雑化すれば乱数生成パターンの不正な解読を有効に防止することができるが、回路のサイズが大きくなってしまう。特に非接触ＩＣカードの場合、内蔵する乱数生成回路のサイズは小さいほうが好ましい。

【００１１】非接触ＩＣカードは、リーダ／ライタと通信可能な領域にある間に相互認証処理を含む通信処理を完了する必要がある。このため、スロットに差し込んで使用するＩＣカードよりも高速な通信処理の実行が要求される。また、非接触ＩＣカードの場合、リーダ／ライタと通信可能な領域内に同時に複数の非接触ＩＣカードが入り込むことがある。この場合、各非接触ＩＣカードは、上記相互認証処理を含む通信処理の実行前に、例えば内部で生成した乱数に基づくタイミングでリーダ／ライタからのポーリング信号に対するレスポンス信号を出力する等、他の非接触ＩＣカードから出力されるレスポンス信号との衝突を回避する処理を実行する必要がある。非接触ＩＣカードとリーダ／ライタ間の通信速度を向上するには、高速で動作する乱数生成回路が要求される。

【００１２】本発明は、簡単な構成で当該回路を内蔵する装置の小型化に寄与し、かつ、高速に規則性の無い予測の困難な乱数データを発生する乱数生成回路、当該乱数生成回路を内蔵する非接触ＩＣカード、及び、当該乱数生成回路を内蔵する非接触ＩＣカード用リーダ／ライタを提供することを目的とする。

【００１３】

【課題を解決するための手段】本発明の第１の乱数生成回路は、カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の２以上のシフトレジスタの出力の合計を求め、求めた合計の

データを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、上記複数のシフトレジスタの内の１以上のシフトレジスタは、外部信号入力端子と、格納しているビットデータの内の１以上のビットデータに上記外部信号入力端子を介して入力されるビットデータを加算する加算回路とを備え、加算回路による加算後のビットデータを乱数データとして出力することを特徴とする。

【００１４】本発明の第２の乱数生成回路は、カスケード接続された複数のクロック同期型シフトレジスタと、上記複数のシフトレジスタの内の２以上のシフトレジスタの出力の合計を求め、求めた合計のデータを初段のシフトレジスタの入力端子に入力する回路と、上記各シフトレジスタにクロック信号を入力するクロック発生回路とを備え、各シフトレジスタの出力するビットデータを乱数データとして出力する乱数生成回路であって、上記クロック発生回路は、所定の周波数のクロック信号を生成するＣＬＫ回路と、上記ＣＬＫ回路により生成されたクロック信号を基準周波数信号として受け取るＰＬＬ回路とで構成され、上記ＰＬＬ回路の出力を上記各シフトレジスタに出力することを特徴とする。

【００１５】本発明の第３の乱数生成回路は、上記第１又は第２の乱数生成回路において、上記シフトレジスタを構成するクロック同期型のフリップフロップは、電源投入時に出力するデータを”Ｈ”とする第１構成要素と、第１構成要素と同一のドライブ能力を有し電源投入時に出力するデータを”Ｌ”とする第２構成要素とを備え、上記第１及び第２構成要素の出力端子には、それぞれ同一の容量の配線及びトランジスタが接続されていることを特徴とする。

【００１６】本発明の第４の乱数生成回路は、上記第１乃至第３の何れかの乱数生成回路において、更に、リセット要求信号の入力に応じて各シフトレジスタにリセット信号を出力するリセット回路を備え、上記クロック発生回路は、クロック停止信号の入力に応じてクロック信号の各シフトレジスタへの出力を停止し、クロック動作信号の入力に応じてクロック信号を各シフトレジスタへ出力する論理回路を備えることを特徴とする。

【００１７】本発明の非接触ＩＣカードは、上記第１乃至第４の何れかの乱数生成回路を内蔵する非接触ＩＣカードであって、当該非接触ＩＣカード用リーダ／ライタとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする。

【００１８】本発明のリーダ／ライタは、上記第１乃至第４の何れかの乱数生成回路を内臓する、非接触ＩＣカード用リーダ／ライタであって、対応する非接触ＩＣカードとの間で、上記内蔵する乱数生成回路から出力される乱数データを用いて通信処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されていることを特徴とする。

【００１９】上記第４の乱数生成回路を内臓し、当該内蔵する乱数生成回路から出力される乱数データを用いて所定の処理を実行する制御手段を備え、上記制御手段により使用される所定の信号線が上記外部信号入力端子に接続されている装置のテスト方法であって、クロック発生回路の論理回路にクロック停止信号を出力すると共に、リセット回路にリセット要求信号を出力した後に、クロック発生回路の論理回路にクロック動作信号を出力すると同時に上記装置のテスト処理を実行し、上記テスト処理の完了と同時にクロック発生回路の論理回路にクロック停止信号を出力し、出力手段より出力される乱数データの値を読み取り、読み取った乱数データと基準データとの比較により、システムの異常検出を行い、上記内蔵する乱数生成回路をテスト回路として利用する。これにより、テスト専用の回路を不要にして装置の小型化を図ることができる。

【００２０】

【発明の実施の形態】以下、実施の形態に係る乱数生成回路、当該乱数生成回路を内蔵する非接触ＩＣカード、及び、当該乱数生成回路を内蔵する非接触ＩＣカード用リーダ／ライタについて、添付の図面を参照しつつ説明する。

【００２１】（１）非接触ＩＣカード

本実施の形態に係る乱数生成回路を内蔵する非接触ＩＣカードは、例えば、地下鉄の自動改札システムに採用することを想定している。より具体的には、図１に示すように、自動改札機として機能するリーダ／ライタ４００の前を、例えば定期券や回数券としての機能を有する非接触ＩＣカード１００，２００，３００を有する人が順に通過する場合を想定する。リーダ／ライタ４００は、前を通過する際に通信エリア内に入る非接触ＩＣカード１００，２００，３００を順に認識し、定期券か回数券の種別についての情報、カードが定期券の場合には有効期限などの情報、及び、カードが回数券の場合には残りの枚数などの情報を読み取り、更に、必要に応じて各カードの情報を更新する。

【００２２】（２）非接触ＩＣカードの認証

リーダ／ライタ４００は、自己の発信するポーリング信号に対して所定のレスポンス信号を返信してきた非接触ＩＣカードとの間で相互認証処理を実行する。図２は、非接触ＩＣカード１００とリーダ／ライタ４００との間で行われる相互認証処理のシーケンスを示す図である。まず、リーダ／ライタ４００から非接触ＩＣカード１００に対して内蔵する乱数生成回路により生成した認証用乱数ａを送信する（ステップＳ１）。通信エリア内において認証用乱数ａを受信した非接触ＩＣカード１００

は、自己の暗号化鍵を用いて乱数ａを乱数Ａに変換し、乱数Ａをリーダ／ライタ４００に対して返信すると共に、内蔵する乱数生成回路により生成した認証用乱数ｂを送信する（ステップＳ２）。リーダ／ライタ４００は、アクセスを行う非接触ＩＣカードと共通に用いる暗号化鍵を用いて乱数ａを乱数Ａ’に変換し、乱数Ａ’と非接触ＩＣカード１００から返信されてきた乱数Ａとが一致する場合に非接触ＩＣカード１００を認証する。また、非接触ＩＣカード１００より送信されてきた乱数ｂを自己の暗号化鍵を用いて乱数Ｂに変換し、乱数Ｂを非接触ＩＣカード１００に対して返信する（ステップＳ３）。非接触ＩＣカード１００は、アクセスを行うリーダ／ライタと共通に用いる暗号化鍵を用いて乱数ｂを乱数Ｂ’に変換し、乱数Ｂ’と返信されてきた乱数Ｂとが一致する場合にリーダ／ライタ４００を認証する（ステップＳ４）。

【００２３】（３）非接触ＩＣカード及びリーダ／ライタの構成

図３は、非接触ＩＣカード１００及びリーダ／ライタ４００のブロック構成図である。なお、非接触ＩＣカード２００，３００の構成は、非接触ＩＣカード１００と同じであり、重複した説明は省略する。

【００２４】非接触ＩＣカード１００は、電池レスタイプの非接触ＩＣカードである。電源回路１８０は、リーダ／ライタ４００から送信される高周波信号をアンテナ１０１により受信し、受信した高周波信号を整流して得られる信号を電圧Ｖｃｃの供給信号としてクロック発生回路１３０を含む各内部回路に供給する。電源回路１８０の構成については後に説明する。

【００２５】クロック発生回路１３０は、上記電源回路１８０から供給される電圧Ｖｃｃにより駆動され、クロック信号ＣＬＫを中央演算処理装置であるＣＰＵ１０３、乱数生成回路１０７を構成するランダムビット生成回路１１０、及び、その他の回路素子に出力する。クロック発生回路１３０の構成については後に説明する。

【００２６】ＣＰＵ１０３には、システムバス１７０を介して送受信回路１０２、ＲＯＭ１０４、ＲＡＭ１０５、情報記憶部１０６、及び、乱数生成回路１０７が接続されている。送受信回路１０２は、アンテナ１０１に接続されており、ＣＰＵ１０３から送られてくる命令やデータを載せた高周波信号をアンテナ１０１を介して外部に発信すると共に、アンテナ１０１を介して受信した高周波信号から命令やデータを抽出してＣＰＵ１０３に出力する処理を行う。ＲＯＭ１０４は、リーダ／ライタ４００との相互認証処理等の通信処理を実行するプログラムを格納する。ＲＡＭ１０５は、ＲＯＭ１０４に格納するプログラムのＣＰＵ１０３による実行時に使用される。情報記録部１０６は、独自の情報、例えば非接触ＩＣカード１００が定期券として機能する場合、カードの有効期限や有効乗車エリアなどの固有の情報を保持する。ＣＰＵ１０３は、リーダ／ライタ４００との通信処理の実行に伴い、必要に応じて上記情報記録部１０６に記憶する情報の更新を行う。乱数生成回路１０７は、ＣＰＵ１０３による所定のアドレスの選択に応じてリーダ／ライタ４００との相互認証処理等で用いる乱数データを上記ＣＰＵ１０３に出力する。

【００２７】乱数生成回路１０７は、デコーダ１０８、ランダムビット生成回路１１０及びリセット回路１４０で構成される。デコーダ１０８は、ＣＰＵ１０３のシステムバス１７０を介して入力されるアドレス信号のデータをデコードしてランダムビット生成回路１１０に出力する。ランダムビット生成回路１１０は、システムバス１７０に流れるアドレス信号のデータ、データ信号のデータ及びその他の信号のデータが内部で生成する乱数データを複雑化するために入力され、上記デコーダ１０８を介して所定のアドレスの選択された場合に合計で３バイト（４８ビット）の乱数データをＣＰＵ１０３に出力する。リセット回路１４０は、ＣＰＵ１０３の制御に応じて所定のリセット信号をランダムビット生成回路１４０に出力する。なお、ランダムビット生成回路１１０及びリセット回路１４０の構成については後に詳しく説明する。

【００２８】リーダ／ライタ４００は、アンテナ４０１、上記アンテナ４０１を用いて命令やデータが載った高周波信号の送受信を行う送受信回路４０２、中央演算処理装置であるＣＰＵ４０３、上記非接触ＩＣカード１００との相互認証処理を含む通信プログラムを格納しているＲＯＭ４０４、ＣＰＵ４０３によるプログラム実行時に使用されるＲＡＭ４０５、インターフェース４０６、及び、乱数生成回路４０７より構成される。なお、乱数生成回路４０７は、非接触ＩＣカード１００に内蔵する乱数生成回路１０７と同じ構成である。

【００２９】リーダ／ライタ４００において、中央演算処理装置であるＣＰＵ４０３は、システムバスを介して送受信回路４０２、ＲＯＭ４０４、ＲＡＭ４０５、インターフェース４０６及び乱数生成回路４０７に接続されている。送受信回路４０２は、接続されるアンテナ４０１を介して受信した高周波信号から命令やデータを抽出してＣＰＵ４０３に出力すると共に、ＣＰＵ４０３からの命令やデータを載せた高周波信号をアンテナ４０１を介して発信する。ＣＰＵ４０３は、例えば非接触ＩＣカード１００との相互認証処理の実行時に、乱数生成回路４０７から得られる乱数データを用いる。ＣＰＵ４０３は、通信処理の結果をインターフェース４０６を介して各処理装置へ出力する。

【００３０】図４は、電源回路１８０の構成を示す図である。電源回路１８０は、整流回路を構成するダイオード１８１、１８２、１８３及び１８４、並びに、容量１８５で構成される。当該整流回路は、アンテナ１０１を介して入力される高周波信号の整流を行い、当該整流後

の信号を電圧供給信号として各内部回路に出力する。

【００３１】図5は、リーダ／ライタ４００からの高周波信号の受信開始から電源回路１８０から出力される電圧供給信号の電位の変化を示すグラフである。図示するように、電源回路１８０から出力される電圧供給信号の電位が規定値Ｖｃｃになるには、高周波信号の受信を開始してから所定の時間が必要である。なお、電圧供給信号の電位がＶｃｃとなるまでに要する時間は、リーダ／ライタ４００との通信環境により変化する。

【００３２】（４）乱数生成回路

図6は、乱数生成回路１０７に内蔵されるランダムビット生成回路１１０及びリセット回路１４０、並びに、クロック発生回路１３０の詳細な構成を示す図である。

【００３３】(4-1)ランダムビット生成回路

ランダムビット生成回路１１０は、いわゆる４８ビットM系列乱数生成回路を構成する１ビットシフトレジスタ１１１，２ビットシフトレジスタ１１５，２５ビットシフトレジスタ１２２、及び、２０ビットシフトレジスタ１２３に格納される各ビットデータに、ＣＰＵ１０３の実行する処理の内容により時間と共に変化するビットデータ、具体的には、システムバス１７０を通る２０ビットのアドレス信号の各ビットデータＡ０～Ａ１９、１６ビットのデータ信号の各ビットデータＤ０～Ｄ１５、及び、その他の信号で構成される計１２ビットの各ビットデータを各々加算し、加算して得られる３バイト、即ち計４８ビットのデータD_10～D_115，D_20～D_215，D_30～D_315を乱数データとして出力する構成を採用したことを特徴とする。

【００３４】上記構成を採用することで、規則性の無い予測の困難な乱数データを生成することができる。これにより、非接触ＩＣカード１００とリーダ／ライタ４００との間で行われる通信データを盗聴しても乱数の生成パターンを特定することが難しくなり、非接触ＩＣカードの偽造を有効に防止することができる。また、ランダムビット生成回路１１０は、シフトレジスタ及び加算器（ＥＸＯＲゲート）を接続しただけの簡単な構成を採用するため、高速な乱数の生成を行うことができる。

【００３５】以下、ランダムビット生成回路１１０の構成について詳説する。ランダムビット生成回路１１０は、カスケード（多段直列）接続された１ビットシフトレジスタ１１１、２ビットシフトレジスタ１１５，２５ビットシフトレジスタ１２２及び２０ビットシフトレジスタ１２３、並びに、各シフトレジスタの出力の合計を初段の２０ビットシフトレジスタ１２３に出力する回路を構成する３つの加算器１２４，１２５，１２６で構成される。

【００３６】２０ビットシフトレジスタ１２３の入力端子は加算器１２６の出力端子に接続される。２０ビットシフトレジスタ１２３の出力端子は加算器１２６の入力端子及び２５ビットシフトレジスタ１２２の入力端子に接続される。２５ビットシフトレジスタ１２２の出力端子は、加算器１２５の入力端子及び２ビットシフトレジスタ１１５の入力端子に接続される。２ビットシフトレジスタ１１５の出力端子は、加算器１２４の入力端子及び１ビットシフトレジスタ１１１の入力端子に接続される。１ビットシフトレジスタ１１１の出力端子は、加算器１２４の入力端子に接続される。加算器１２４の出力端子は加算器１２５の入力端子に接続される。加算器１２５の出力端子は加算器１２６の入力端子に接続される。

【００３７】１ビットシフトレジスタ１１１は、デコーダ１０８を介してアドレス１５Ｆ２Ｈが選択され、対応するアドレス信号線が”Ｌ”から”Ｈ”に切り換わった時に、格納する１ビットデータに、システムバス１７０を流れる１６ビットのデータ信号のｂｉｔ０のデータＤ０を加算して得られるデータのｂｉｔ０のデータD_10を乱数データとして出力する。

【００３８】１ビットシフトレジスタ１１１は、加算器１１２、フリップフロップ１１３、トランスファーゲート１１４で構成されている。加算器１１２は、例えばＥＸＯＲゲートで構成され、前段に設けられる２ビットシフトレジスタ１１５の出力に、システムバス１７０を介して入力される１６ビットデータ信号のｂｉｔ０のデータＤ０を加算して得られるｂｉｔ０のデータをフリップフロップ１１３に入力する。フリップフロップ１１３は、クロック同期型のフリップフロップであり、クロック入力端子に入力されるクロック信号ＣＬＫの遷移タイミングに同期して動作する。トランスファーゲート１１４は、アドレス１５Ｆ２Ｈが選択され、対応するアドレス信号線が”Ｌ”から”Ｈ”に切り換わった時に、フリップフロップ１１３の出力Ｑを乱数データD_10として出力する。

【００３９】２ビットシフトレジスタ１１５は、デコーダ１０８を介してアドレス１５Ｆ２Ｈが選択され、対応するアドレス信号線が”Ｌ”から”Ｈ”に切り換わった時に、格納している２ビットの各ビットデータに、データバスを介して入力される１６ビットデータ信号のｂｉｔ２のデータＤ２及びｂｉｔ１のデータＤ１を加算したデータD_11及びD_12を乱数データとして出力する。

【００４０】図示するように、２ビットシフトレジスタ１１５は、１ビットシフトレジスタを２段直列に接続したものである。即ち、加算器１１６、フリップフロップ１１７、及び、トランスファーゲート１１８で１つ目の１ビットシフトレジスタを構成し、次の加算器１１９、フリップフロップ１２０、及び、トランファーゲート１２１で２つ目の１ビットシフトレジスタを構成する。以下に説明する２５ビットシフトレジスタ１２２及び２０ビットシフトレジスタ１２３も同様である。各シフトレジスタ内における信号の処理内容は上記１ビットシフトレジスタ１１１と同様であるため、ここでの説明は省

略する。

【００４１】２５ビットシフトレジスタ１２２は、格納している２５ビットの各ビットデータに、アドレスバスを介して入力される２０ビットのアドレス信号のｂｉｔ０～ｂｉｔ１１の各ビットデータＡ０～Ａ１１、及び、データバスを介して入力される１６ビットのデータ信号のｂｉｔ３～ｂｉｔ１５の各ビットデータＤ３～Ｄ１５を加算して得られる２５ビットのビットデータ$D_1$３～$D_1$７，$D_1$８～$D_1$１５，$D_2$０～$D_2$７及び$D_2$８～$D_2$１１を、アドレス１５Ｆ２Ｈ，１５Ｆ３Ｈ，１５Ｆ４Ｈ及び１５Ｆ５Ｈの選択に応じて出力する。

【００４２】２０ビットシフトレジスタ１２３は、格納されている２０ビットの各ビットデータに、データ信号及びアドレス信号以外の信号で構成される８ビットの各ビットデータｂｉｔ０～ｂｉｔ７の各ビットデータＲｅｖ０～Ｒｅｖ７、及び、アドレスバスを介して入力される２０ビットのアドレス信号のｂｉｔ１２～ｂｉｔ１９の各ビットデータＡ１２～Ａ１９を加算した２０ビットのデータ$D_2$１２～$D_2$１５，$D_3$０～$D_3$７及び$D_3$８～$D_3$１５を、アドレス１５Ｆ５Ｈ，１５Ｆ６Ｈ及び１５Ｆ７Ｈの選択に応じて出力する。

【００４３】上述するように、ランダムビット生成回路１１０では、各ビットシフトレジスタ１１１，１１５，１２２及び１２３内に格納する各ビットデータに対して、システムバス１７０を流れるアドレス信号、データ信号及びその他の信号を構成する各ビットデータを加算する構成を採用する。システムバス１７０に流れる信号の値は、実行する処理内容に伴い種々変化するため、規則性の無い予測の困難な乱数データを生成することができる。これにより、非接触ＩＣカード１００とリーダ／ライタ４００との間で交わされる通信データを盗聴しても乱数の生成パターンを特定することは難しくなり、非接触ＩＣカードの偽造を有効に防止することができる。また、ランダムビット生成回路１１０は、シフトレジスタ及び加算器（ＥＸＯＲゲート）を接続しただけの簡単な構成であるため、高速な乱数の生成を行うことができる。

【００４４】上記ランダムビット生成回路１１０は、カスケード接続した全てのシフトレジスタの出力の合計を初段の２０ビットシフトレジスタ１２３の入力端子に入力する構成を採用するが、これに限定されず、ランダムビット生成回路１１０を構成する４つのシフトレジスタの内の２以上のシフトレジスタの出力の合計を初段の２０ビットシフトレジスタ１２３の入力端子に入力する構成であれば良い。

【００４５】また、ランダムビット生成回路１１０は、ＣＰＵ１０３による所定のアドレスの選択に対応して全てのシフトレジスタに格納するビットデータを乱数データとして出力する構成を採用するが、これに限定されず、１以上のビットデータを出力する構成であれば良い。

【００４６】更に、ランダムビット生成回路１１０は、各シフトレジスタに格納する全てのビットデータにシステムバス１７０のビットデータを加算する構成を採用しているが、これに限定されず、シフトレジスタに格納しているビットデータの内の１以上のビットデータにシステムバス１７０のビットデータを加算する構成であれば良い。

【００４７】(4-2)リセット回路

リセット回路１４０は、２入力ＮＡＮＤゲート１４１で構成される。ＮＡＮＤゲート１４１の入力端子にはアドレス１５Ｆ１Ｈのアドレス信号線が接続され、残りの入力端子には書き込み命令が出された場合に”Ｌ”から”Ｈ”に切り換わるＷ信号線が接続されている。ＣＰＵ１０３は、アドレス１５Ｆ１Ｈに対してデータの書き込みを行うことで、ランダムビット生成回路１１０を構成する各シフトレジスタ１１１，１１５，１２２，１２３のリセットを行うことができる。

【００４８】(4-3)クロック発生回路

図６に示すように、クロック発生回路１３０は、ＣＬＫ回路１３１、ＰＬＬ１３２、及び、ＮＡＮＤゲート１３３で構成される。ＣＬＫ回路１３１は、電源回路１８０から電圧供給信号が出力されると同時に、所定の周期のクロック信号を基準周波数信号として次段のＰＬＬ回路１３２に出力する。周知のように、ＰＬＬ回路１３２は、上記基準周波数信号の周波数に収束するまでの間、電源回路１８０から出力される電圧供給信号の電位に比例して決まる周波数のクロック信号を出力する。ＰＬＬ回路１３２の出力端子は、２入力ＮＡＮＤゲート１３３の一方の入力端子に接続されている。ＮＡＮＤゲート１３３のもう一方の入力端子には、デコード後のアドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０が入力される。通常、アドレス１５Ｆ０Ｈのデータｂ０は”Ｌ”に設定されており、ＮＡＮＤゲート１３３は、ＰＬＬ回路１３１からのクロック信号ＣＬＫの反転信号をランダムビット生成回路１１０を構成する各シフトレジスタ１１１、１１５、１２２及び１２３に出力する。

【００４９】上述するように、クロック発生回路１３０の出力するクロック信号の周波数は、電源回路１８０から出力される電圧供給信号の電位により決まる。このため、電源回路１８０から出力される電圧供給信号の電位が規定値Ｖｃｃに安定するまでの間は、全く同じタイミングで乱数データの読み取りを行っても、ランダムビット生成回路１１０から出力される乱数データの値は異なる。また、非接触ＩＣカード１００と全く同じ構成の非接触ＩＣカード２００や３００であっても、各構成部品のばらつきにより上記乱数データの読み取りタイミングは微妙に異なるため、電源投入直後にランダムビット生成回路１１０から出力される乱数データは各カード毎に異なる。このように上記構成のクロック発生回路１３０

を採用することで、通信データの盗聴による乱数データの発生パターンの特定を一層難しくすることができる。

【００５０】なお、上記構成のクロック発生回路１３０において、ＣＰＵ１０３によりアドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０が”Ｌ”から”Ｈ”に書き換えられると、ＮＡＮＤゲート１３３は”Ｈ”のみを出力する。これにより、ランダムビット生成回路１１０を構成する各シフトレジスタ１１１、１１５、１２２及び１２３へのクロック信号の出力は停止し、各シフトレジスタの機能は停止する。また、アドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０の値を”Ｈ”から”Ｌ”に書き換えることで、各シフトレジスタへのクロック信号の出力を再開することができる。このように、ＣＰＵ１０３は、ランダムビット生成回路１１０を動作及び停止することができる。

【００５１】(4-4)フリップフロップ

１ビットシフトレジスタ１１１を構成するクロック同期型フリップフロップ１１３は、電源投入時に出力するデータを”Ｈ”とする第１構成要素と、上記第１構成要素と同じドライブ能力を備え、電源投入時に出力するデータを”Ｌ”とする第２構成要素を備えると共に、上記第１及び第２構成要素の出力端子に接続される配線容量を同じにしたことを特徴とする。これにより、電源投入時に出力されるデータが”Ｈ”又は”Ｌ”となる確率を５０％にする。

【００５２】図７は、フリップフロップ１１３の構成を示す図である。２入力ＯＲゲート１５０の一方の入力端子は、クロック信号ＣＬＫの入力端子に接続されており、他方の入力端子はデータ信号Ｄの入力端子に接続されている。ＯＲゲート１５０の出力端子は２入力ＮＡＮＤゲート１５１の一方の入力端子に接続されている。ＮＡＮＤゲート１５１の出力端子は、２入力ＮＡＮＤゲート１５３の一方の入力端子、ゲート電極及びソース電極が接地されているＮチャンネルＭＯＳトランジスタ１５９のドレイン電極、及び、２入力ＡＮＤゲート１５４の一方の入力端子に接続されている。２入力ＯＲゲート１５２の一方の入力端子は、クロック信号ＣＬＫの入力端子に接続されており、他方の入力端子はインバータ１６０を介してデータ信号Ｄの入力端子に接続されている。ＯＲゲート１５２の出力端子は、２入力ＮＡＮＤゲート１５３の一方の入力端子に接続されている。ＮＡＮＤゲート１５３の出力端子は、ＮＡＮＤゲート１５１の残りの入力端子、ＮチャンネルＭＯＳトランジスタ１５８のドレイン電極、及び、２入力ＡＮＤゲート１５６の一方の入力端子に接続される。ＮチャンネルＭＯＳトランジスタ１５８のゲート電極にはリセット端子が接続されている。ＮＯＲゲート１５５の出力端子は、データＱの出力端子、及び、ＮＯＲゲート１５７の入力端子に接続される。ＮＯＲゲート１５７の出力端子は、データＱの反転信号ＱＢの出力端子、及び、ＮＯＲゲート１５５の入力端子に接続される。

【００５３】上記構成のフリップフロップ１１３において、電源投入時に出力するデータの値に影響を与える構成要素であるＮＡＮＤゲート１５１及び１５３は、同一のドライブ能力のものを採用する。また、当該ＮＡＮＤゲート１５１と１５３の出力端子に接続される配線容量が同一となるように、ＮＡＮＤゲート１５１と１５３の出力端子に接続される配線長を同一に設計すると共に、リセット端子の接続されるＮチャンネルＭＯＳトランジスタ１５８により配線に付加される容量を補償するためＭＯＳトランジスタ１５８と同一規格のＭＯＳトランジスタ１５９を対応箇所に設ける。これにより、電源投入時にフリップフロップ１１３から出力端子Ｄに出力される信号の値が”Ｈ”又は”Ｌ”である確率を５０％にすることができる。

【００５４】ランダムビット生成回路１１０では、上記フリップフロップ１１３と同じ構成のフリップフロップを２ビットシフトレジスタ１１５、２５ビットシフトレジスタ１２２及び２０ビットシフトレジスタ１２３にも採用する。これにより、非接触ＩＣカード１００の起動時に各シフトレジスタから偏りの無い初期値が出力されるため、乱数データの予測を一層難しくすることができる。

【００５５】（５）乱数生成処理

以下、上記構成の乱数生成回路１１０を用いてＣＰＵ１０３の実行する乱数生成処理の内容について説明する。図８は、乱数生成処理のフローチャートである。まず、アドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０を”０”にセットする（ステップＳ５）。これにより、クロック発生回路１３０からのクロック信号ＣＬＫの出力が停止し、これに伴いランダムビット生成回路１１０の動作が停止する。アドレス１５Ｆ２Ｈ～１５Ｆ７Ｈを選択し、対応するアドレス信号線を”Ｌ”から”Ｈ”に切り換え、データD_10～D_115，D_20～D_215，D_30～D_315を乱数データとして読み出す（ステップＳ６）。更に別の乱数が必要な場合（ステップＳ７でＹＥＳ）、アドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０を”１”にセットして、ランダムビット生成回路１１０を始動させた後に（ステップＳ８）、上記ステップＳ５に戻る。これ以上の乱数が不要の場合には（ステップＳ７でＮＯ）、処理を終了する。上記乱数生成処理を実行することで、ＣＰＵ１０３は、乱数生成回路１１０において所定のタイミングで生成された乱数データを抽出することができる。

【００５６】（６）テスト処理

上述するように、乱数生成回路１０７は、システムバス１７０を流れるデータを利用して規則性の無い予測の困難な乱数を生成することを特徴とする。ところで、所定の周波数のクロック信号ＣＬＫが入力されている状態において、ランダムビット生成回路１１０をリセットした

後に、非接触ＩＣカード１００のテスト処理を実行した場合を想定する。回路が正常な場合には、テスト処理の実行直後にランダムビット生成回路１１０から出力される乱数データは常に一定の値となる。当該特性を利用すれば、乱数生成回路１０７を非接触ＩＣカード１００の動作テスト装置として利用することができる。乱数生成回路１０７をテスト装置として利用することで、テスト専用の回路を不要にして非接触ＩＣカード１００の小型化を図ることができる。

【００５７】図９は、ＣＰＵ１０３がランダムビット生成回路１１０を利用して行うテスト処理のフローチャートである。まず、クロック発生回路１３０のＰＬＬ回路１３３に電源回路１８０から供給される電圧供給信号の電位が規定値Ｖｃｃに安定し、所定の周波数のクロック信号ＣＬＫが安定して出力される状態で、アドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０を”０”にセットして、クロック発生回路１３０の動作を停止、即ち、ランダムビット回路１１０の動作を停止する（ステップＳ１０）。アドレス１５Ｆ１Ｈにダミーデータを書き込み、書き込み命令Ｗの値を”Ｌ”から”Ｈ”に切り換え、リセット回路１４０を機能して各シフトレジスタ１１１，１１５，１２２，１２３内のデータ（アドレス１５Ｆ２Ｈ～１５Ｆ７Ｈのデータ）をクリアする（ステップＳ１１）。１５Ｆ０Ｈのｂｉｔ０のデータｂ０を”１”にセットして、クロック発生回路１３０を始動させる（ステップＳ１２）。ＲＯＭ１０４に記憶するテスト用プログラムを実行する（ステップＳ１３）。テスト用プログラムの実行完了後、アドレス１５Ｆ０Ｈのｂｉｔ０のデータｂ０を”０”にセットし、クロック発生回路１３０の動作を停止する（ステップＳ１４）。アドレス１５Ｆ２Ｈ～１５Ｆ７Ｈを選択して対応するアドレス信号線を”Ｌ”から”Ｈ”に切り換え、各ビットデータ$D_1$０～$D_1$１５，$D_2$０～$D_2$１５，$D_3$０～$D_3$１５を読み出す（ステップＳ１５）。

【００５８】内部の回路が正常の場合、上記ステップＳ１５において読み出した各ビットデータ$D_1$０～$D_1$１５，$D_2$０～$D_2$１５，$D_3$０～$D_3$１５の値は一定の値を示す。そこで、上記ステップＳ１５で読み出した各ビットデータの値と各ビットデータの基準値、例えば、前回読み出した各ビットデータの値又は予め記憶している各ビットデータの値との比較を行い、回路内部に何等かの不都合が生じているか否かの判断を行う（ステップＳ１６）。比較の結果、上記読み出した各ビットデータの値が基準値と同じ場合には正常であると判断して処理を終了する（ステップＳ１６でＹＥＳ）。一方、上記読み出した各ビットデータが１つでも基準値と異なる場合には回路内に異常があると判断し（ステップＳ１６でＮＯ）、内部データの保護等の異常対策処理（ステップＳ１７）を実行した後に処理を終了する。

【００５９】以上に説明するように、乱数生成回路１０７は、システムバス１７０を介して入力されるアドレス信号、データ信号などの各ビットデータの値を利用して乱数を生成するため、規則性の無い予測の困難な乱数データを生成することができる。また、シフトレジスタと加算器からなる簡単な構成のランダムビット生成回路１１０を採用することで、回路の小型化、及び、高速な乱数生成を実現する。更に、上記ランダムビット生成回路１１０を非接触ＩＣカード１００のテスト装置として利用することで、専用のテスト回路を排除し、非接触ＩＣカード１００の小型化を図ることができる。

【００６０】なお、リーダ／ライタ４００は、非接触ＩＣカード１００の備える乱数生成回路１０７と同じ構成の乱数生成回路４０７を備える。このため、リーダ／ライタ４００でも上記非接触ＩＣカード１００と同様に、規則性の無い予測の困難な乱数データを迅速に生成することができる。更に、乱数生成回路４０７の備えるランダムビット生成回路（図示せず）をリーダ／ライタ４００のテスト装置として利用することで、専用のテスト回路を排除し、リーダ／ライタ４００の小型化を図ることができる。

【００６１】

【発明の効果】本発明の第１の乱数生成回路は、外部信号線に流れるビットデータを利用して乱数データを生成するため、規則性の無い予測の困難な乱数データを生成することができる。また、当該乱数生成回路は、シフトレジスタをカスケード接続してなる簡単な構成であるため、高速な乱数データの生成が可能である。

【００６２】本発明の第２の乱数生成回路では、クロック発生回路に、基準周波数信号と同じ周波数に収束するまでの間、供給される電源電圧の値により決まる周波数のクロック信号を出力するＰＬＬ回路を用いることで、例えば、当該第２の乱数生成回路を内蔵する非接触ＩＣカードでも、各構成部品のばらつき等により電源供給開始直後に出力される乱数データの値を相異させることができる。

【００６３】本発明の第３の乱数生成回路は、上記第１又は第２の乱数生成回路において、更に、各シフトレジスタを構成するクロック同期型フリップフロップの電源投入時に出力するデータを”Ｈ”とする第１構成要素と、”Ｌ”とする第２構成要素のドライブ能力を同じにし、かつ、上記第１及び第２構成要素の出力端子に同じ容量の配線及びトランジスタを接続したことで、電源投入時に出力されるデータが”Ｈ”又は”Ｌ”である確率を５０％にすることができる。これにより、電源の投入時、各シフトレジスタから偏りの無い初期値が出力され、乱数データの予測を一層難しくすることができる。

【００６４】本発明の第４の乱数生成回路は、上記何れかの乱数生成回路において、更に、必要に応じて、クロック信号の出力を停止又は動作させることができる。これにより、所定のタイミングの乱数データの読み取りが

可能になる。また、必要に応じて各シフトレジスタに格納するビットデータをリセットすることができる。

【００６５】本発明の非接触ＩＣカードは、上記何れかの乱数生成回路を備えることで、規則性の無い予測の困難な乱数データを迅速に取得できるため、対応するリーダ／ライタとの間で高速な通信処理を行うことができる。

【００６６】本発明のリーダ／ライタは、上記何れかの乱数生成回路を備えることで、規則性の無い予測の困難な乱数データを迅速に取得できるため、対応する非接触ＩＣカードとの間で高速な通信処理を行うことができる。

【００６７】上記第４の乱数生成回路をテスト装置として利用する本発明のテスト方法を採用すれば、テスト専用の回路が不要となり装置の小型化を図ることができる。

【図面の簡単な説明】

【図１】　リーダ／ライタと非接触ＩＣカードの利用形態を説明するための図である。

【図２】　リーダ／ライタ及び非接触ＩＣカードとの間で実行される相互認証処理のシーケンスを示す図である。

【図３】　リーダ／ライタ及び非接触ＩＣカードのブロック構成図である。

【図４】　電源回路の構成図である。

【図５】　電源回路の出力特性を示すグラフである。

【図６】　ランダムビット生成回路の構成図である。

【図７】　クロック同期型のフリップフロップの構成図である。

【図８】　ＣＰＵの実行する乱数生成処理のフローチャートである。

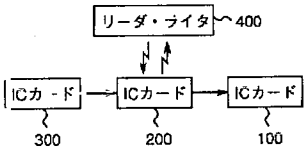
【図９】　ＣＰＵの実行するテスト処理のフローチャートである。

【図１０】　従来の乱数生成回路の構成図である。

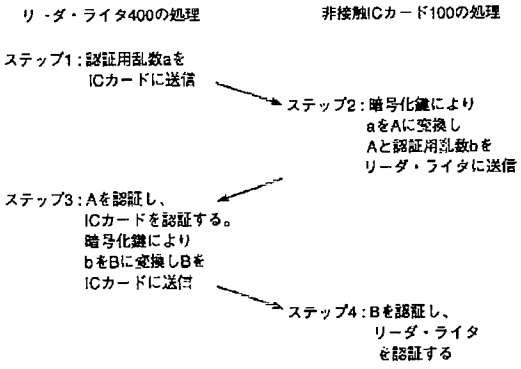
【符号の説明】

１００，２００，３００　非接触ＩＣカード、１０１，４０１　アンテナ、１０２，４０２　送受信回路、１０３，４０３　ＣＰＵ、１０４，４０４　ＲＯＭ、１０５，４０５　ＲＡＭ、１０６　情報記録部、１０７，４０７　乱数生成回路、１０８　電源回路、１１１　1ビットシフトレジスタ、１１２，１１６，１１９，１２４，１２５，１２６　加算器、１１３，１２０，１１７　フリップフロップ、１１４，１１８，１２１　トランスファーゲート、１１５　2ビットシフトレジスタ、１２２　25ビットシフトレジスタ、12320ビットシフトレジスタ、１３０　クロック発生回路、１３１　クロック回路、１３２　ＰＬＬ回路、１３３　ＮＡＮＤゲート、１４０　リセット回路、１４１　ＮＡＮＤゲート、１５０，１５２　ＯＲゲート、１５１，１５３　ＮＡＮＤゲート、１５４，１５６　ＡＮＤゲート、１５５，１５７　ＮＯＲゲート、１５８，１５９　トランジスタ、１７０　システムバス、４００　リーダ／ライタ、４０６　インターフェース

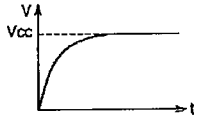
【図１】



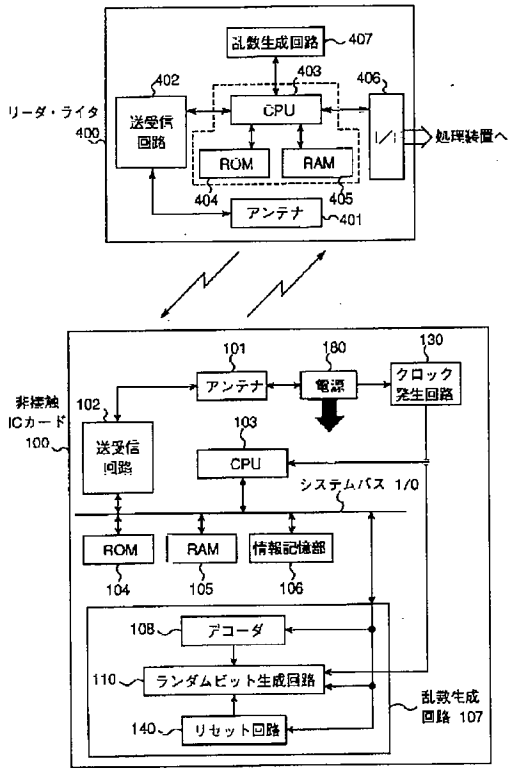
【図２】



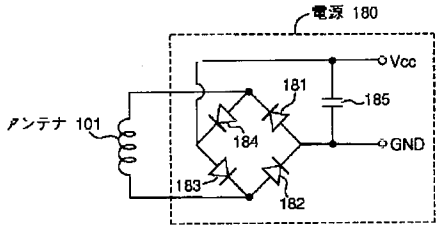
【図５】



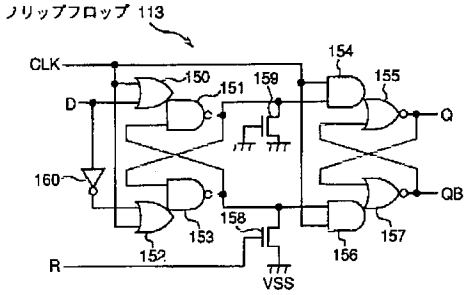
【図3】


乱数生成回路
407
402
403
406
リーダ・ライタ
400
送受信回路
CPU
I/O
処理装置へ
ROM
RAM
404
405
アンテナ
401
非接触ICカード
100
101
180
130
アンテナ
電源
クロック発生回路
102
送受信回路
103
CPU
システムバス I/O
ROM
RAM
情報記憶部
104
105
106
108
デコーダ
110
ランダムビット生成回路
乱数生成回路 107
140
リセット回路

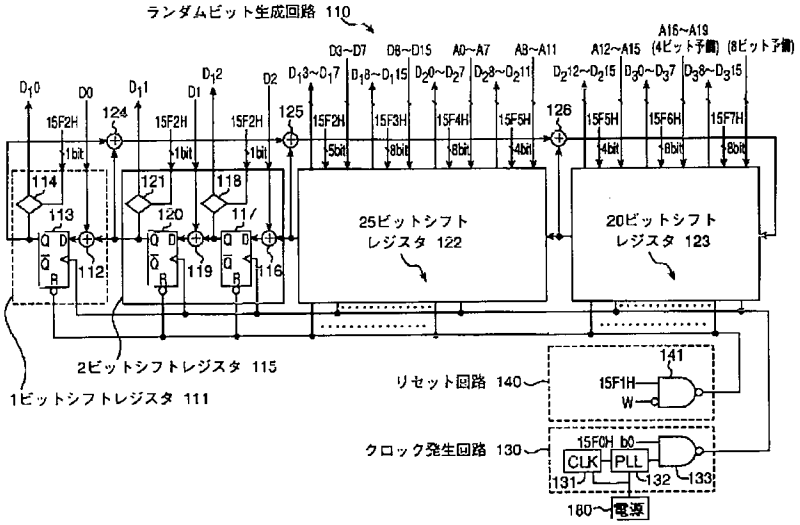
【図4】


電源 180
Vcc
181
185
アンテナ 101
184
GND
183
182

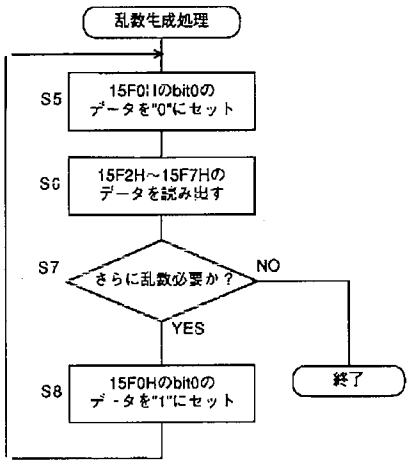
【図7】


フリップフロップ 113
CLK
154
150
151
159
155
D
Q
160
QB
158
153
157
152
156
R
VSS

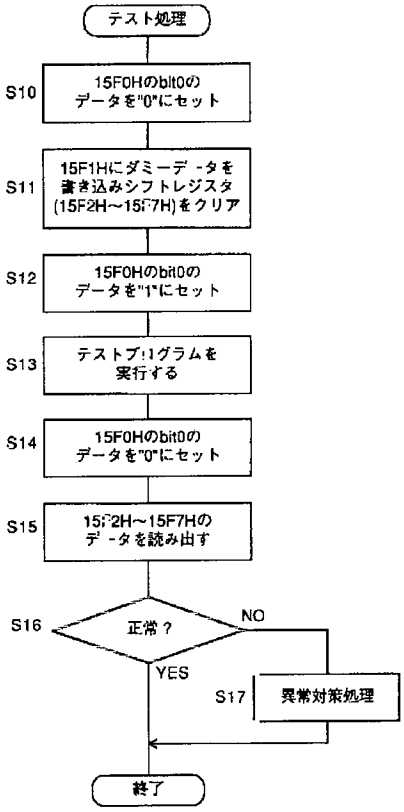
【図6】


ランダムビット生成回路 110
D3~D7
D8~D15
A0~A7
A8~A11
A12~A15
A16~A19
(4ビット予備)
(8ビット予備)
15F2H
15F3H
15F4H
15F5H
15F6H
15F7H
1bit
5bit
8bit
4bit
114
113
121
120
118
117
112
119
116
25ビットシフトレジスタ 122
20ビットシフトレジスタ 123
2ビットシフトレジスタ 115
1ビットシフトレジスタ 111
リセット回路 140
141
15F1H
W
クロック発生回路 130
15F0H b0
CLK
PLL
131
132
133
160
電源

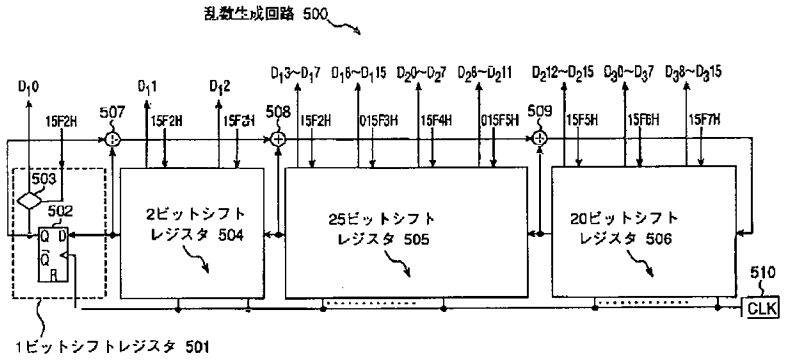
【図8】


乱数生成処理
S5
15F0HのbitOの
データを"0"にセット
S6
15F2H~15F7Hの
データを読み出す
S7
さらに乱数必要か？
NO
YES
S8
15F0HのbitOの
データを"1"にセット
終了

【図9】


テスト処理
S10
15F0HのbitOの
データを"0"にセット
S11
15F1Hにダミーデータを
書き込みシフトレジスタ
(15F2H~15F7H)をクリア
S12
15F0HのbitOの
データを"1"にセット
S13
テストプログラムを
実行する
S14
15F0HのbitOの
データを"0"にセット
S15
15F2H~15F7Hの
データを読み出す
S16
正常？
NO
YES
S17
異常対策処理
終了

【図10】


乱数生成回路 500
D10
15F2H
507
D11
15F3H
D12
508
D13~D17
D18~D115
D20~D27
D28~D211
15F2H
015F3H
15F4H
015F5H
509
D212~D215
D30~D37
D38~D315
15F5H
15F6H
15F7H
503
502
Q
D
R
2ビットシフト
レジスタ 504
25ビットシフト
レジスタ 505
20ビットシフト
レジスタ 506
510
CLK
1ビットシフトレジスタ 501

フロントページの続き

Ｆターム(参考) 5B035 AA00 AA02 AA03 AA04 AA13
BB09 BC02 BC03 CA01 CA08
CA11 CA12 CA22 CA23
5B058 CA17 CA22 CA27 KA08 KA13
KA35 YA06 YA07
5J104 AA18 AA41 FA04 NA23 NA35
9A001 GG22 LL05